

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1272054-0

Total Deleted Page(s) = 8

Page 21 ~ b6; b7C; b7D;
Page 22 ~ b6; b7C; b7D;
Page 23 ~ b6; b7C; b7D;
Page 26 ~ b6; b7C; b7D;
Page 27 ~ b6; b7C; b7D;
Page 38 ~ b6; b7C; b7E;
Page 39 ~ b6; b7C; b7E;
Page 40 ~ b6; b7C; b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/24/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-JK-~~NEW~~ 53354 (Pending) -1Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Synopsis: To open case and document meeting with Lake County Sheriff's Office (LCSO).

Details: On 4/23/2012 SA [REDACTED] and SA [REDACTED] of FBI JK met with [REDACTED] at [REDACTED] Florida 32778 to discuss information that was passed from FBI HQ on 4/21/2012 to SA [REDACTED] about a possible computer intrusion by [REDACTED] into the LCSO network.

[REDACTED] of LCSO was interviewed on 4/23/2012 about a potential intrusion into the LCSO network.

[REDACTED] stated that he had been contacted by an FBI Agent out of San Antonio (SA) and told of a possible computer intrusion back in January of 2012. [REDACTED] stated that he attempted multiple times to reach back out to FBI SA with negative results.

[REDACTED] stated that he believed that the intrusion attempt was un-successful and provided logs and data. Writer and SA [REDACTED] advised [REDACTED] to look again for the possible intrusion by checking server logs and legitimate user accounts for unusual activity and gave him an overview of criminal hacking procedures and techniques. [REDACTED] called Writer back on 4/23/2012 after the meeting to report that he had found a user account that was being accessed for illegitimate purposes and was going to continue the investigation.

UNCLASSIFIED

S:\DRAFTS\ [REDACTED]\115\112.wpd

b6
b7C4/25/12
OgA
SA [REDACTED]

b7E

b6
b7Cb6
b7Cb6
b7C

UNCLASSIFIED

To: Jacksonville From: Jacksonville
Re: 288A-JK-NEW, 04/24/2012

Writer reached out to Cyd HQ, Bucharest ALAT [REDACTED]
[REDACTED], and FBI SA on 4/23/2012 to coordinate the investigation
and collect information pertaining to the possible intrusion at
LCSO. The following is the details of the information that was
provided:

b6
b7C

FBI SA provided the following:

Table name: SO_TBL_USERACCESS

Data:

LCSO,
LCSO,

b6
b7C

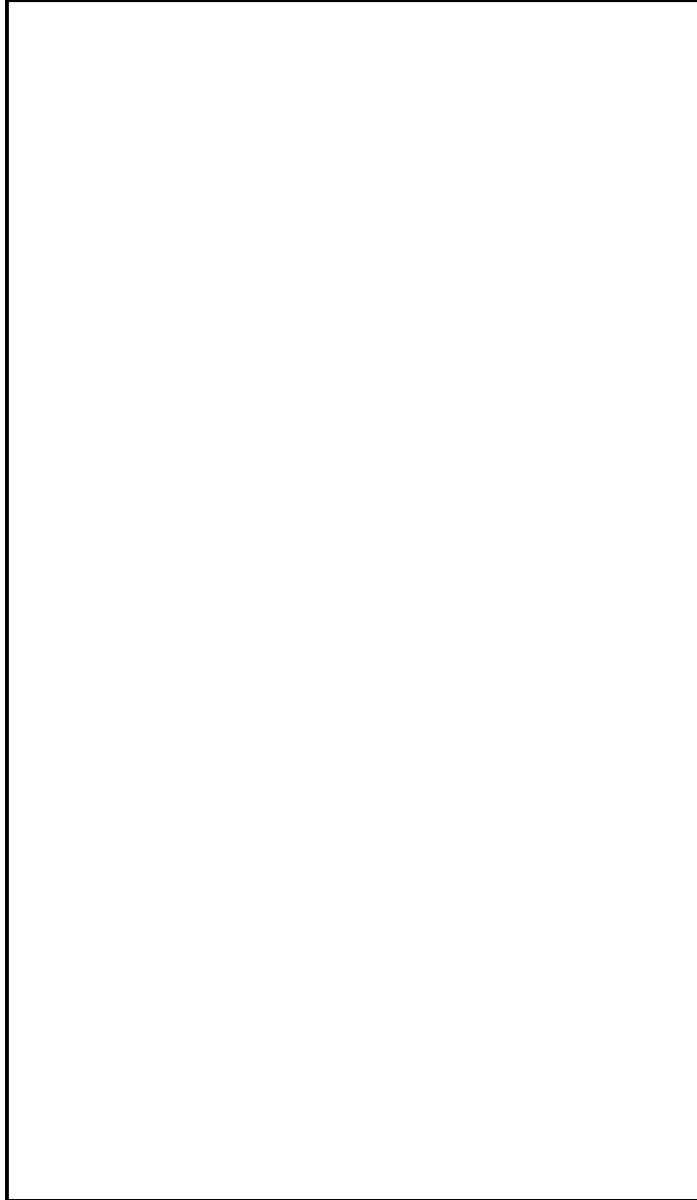
FBI ALAT Bucharest provided the following:

b7D
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Jacksonville From: Jacksonville
Re: 288A-JK-NEW, 04/24/2012



b7D
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Jacksonville From: Jacksonville
Re: 288A-JK-NEW, 04/24/2012

[please note, some of the above may be misspelled]

[redacted]

b6
b7C
b7D

ALAT Bucharest advised that [redacted]
[redacted]

b7D

Based on the above information Writer requests the above
case be opened and assigned to SA [redacted] and Co-Case SA
[redacted]

b6
b7C

♦♦

UNCLASSIFIED

FD-340a (Rev. 1-27-03)

(Title) _____
(File No.) 288A-Jk-53354

FD-340 (Rev. 4-11-03)

File Number 288A-JK-53354-1A

Field Office Acquiring Evidence JK

Serial # of Originating Document 2

Date Received 04/26/2012

From PASTEHTML.COM

(Name of Contributor/interviewee)

(Address)

(City and State)

By SA

b6
b7C

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

PASTEHTML.COM WEB PAGE CONTENT AND
SCREENSHOTS.

FD-340 (Rev. 4-11-03)

File Number 288A-JK-53354

Field Office Acquiring Evidence JK

Serial # of Originating Document _____

Date Received 4/23/12

From (LC50)
(Name of Contributor/interviewee)

360 W Ruby St
(Address)

Tavares, FL 32778

By S A

To Be Returned Yes

Receipt Given Yes No
Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

Federal Rules of Criminal Procedure

Yes

Yes No

Federal Taxpayer Information (FTI)

Yes No

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

Consent to Search Computer), FDS97 Receipt for Property

CART Service Request

b6
b7c

Your Exam service request has been entered into the system and is pending review by the JK office. A representative from the JK office will contact you shortly regarding the status of your request with further information and instructions.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36J55T41/NSICG

Service Request ID: 44687
Request Type: Exam
Request Date: 04/27/2012
Request Priority: 2 (Priority)
Requested Completion Date: 05/02/2012
Investigative Request? Yes
UCFN: 288A - JK - 53354

Case Agent/Investigator: [REDACTED]
Case Agent/Investigator Field Office: JK
Case Agent/Investigator Supervisor: [REDACTED]

Case Title: UNSUB (S); LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Case Synopsis: The Lake County Sheriff's Office was intruded into by [REDACTED] and an estimated 6.2 GB of data was exfiltrated. FBI is working with ALAT [REDACTED]

Submitting Agency: FBI JK

Agency Case/File Number:

Contact Information:

[REDACTED]
6061 Gate Parkway
Jacksonville , FL 32256

Assign Request To: JK

Evidence to be Examined: 1 External HDD containing backups and images of three (3) virtual servers and logs.

Request Description: Copy HDD

Legal Authority: To Be Determined

b6

b7C

b6

b7C

b7D

b6

b7C

b7E

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # _____

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36J55T41/NSICGOn (date) 4/25/2012item(s) listed below were:
 Received From
 Returned To
 Released To
 Seizedb6
b7C(Name) Lake County Sheriff's Office - _____
(Street Address) 360 West Ruby street Tavares, FL 32778
(City) _____Description of Item(s): Western Digital My Book Studio 2TB
Containing backups and Images of
leo app1
leo citrix
APP2 (LEOTTA)As well as logs from leo app1, leo citrix, leo Asp1, website
loggingSerial Number - WCAZ A3188836

Received By: _____

Received From: _____

b6
b7C

FD-340 (Rev. 4-11-03)

File Number 286A-JK-53354 - 1AB

Field Office Acquiring Evidence JK

Serial # of Originating Document 8

Date Received 04/27/2012

From [Redacted]
[Redacted] (Author/interviewee)

b6
b7c

(Address)

(City and State)

By SA [Redacted]

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of
[Redacted]

b6
b7c



DAILY GRIND

Unwind.

Coffee House and Café

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36TJ55T41/NSICG

HELPDESK

@LCSD.ORG

BCC:

9:45 AM

AN IT SEC

INT POTATO

= Ø

UNITE AS ONE

! POTATOES

MAIL SVR DN

4460 Washington Road • Suite 20 • Evans, Georgia 30809
Office 706.854.8838 • Fax 706.854.8022

b6
b7C

FD-340 (Rev. 4-11-03)

File Number 288A-JK-S3354 JA4

Field Office Acquiring Evidence JK

Serial # of Originating Document _____

Date Received 5/29/2012

From ALIT Bucharest
(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA _____

b6

b7C

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

Press Release dated 5/29/2012

PRESS RELEASE
05/29/2012

Prosecutors Department for Organized Crime and Terrorism - Central structure deconstructed a criminal group, consisting of 14 persons, so they carried out 12 house searches in Bucharest, Iasi, Alba Iulia, Piatra Neamt, Cluj Napoca, Turnu Severin, Arad, Craiova and Targu Mures Resita.

Group leader was identified as the accused BĂLĂEASA Gabriel, 24, of Piatra Neamt, known in the virtual environment with nicknames "lulzcart, anonsboat, anonsweb, Cartman."

This, together with Gabor and Picos Fábián accused Michael Emil was a group, joined by other people involved in the cyber terrorist attacks.

The group conducted an extensive criminal activity specific for cybercrime, which consisted of illegal access to computer systems, misuse of confidential or non public and published in the online environment seep data.

Databases confidential / classified subjects were given preference for public institutions and businesses, both in Romania and abroad.

For technical and practical way of operating, cyber attacks launched on the target server and Web pages, were SQL injection, using different applications, namely Havij, SQL, etc. Map. In most cases, after compromise and obtain unauthorized access to targeted sites, the group members brought changes to computer data, executing attacks "deface", consists of applying a web page instead of the main site, which was to change general in certain posting messages, links and images that promote group claims attack and hackers.

Attacks were launched in order to obtain computer data, appropriate data were copied / transferred without the right and subsequently published in the virtual environment on various sites as evidence of hacking activity.

Group members did so to launch attacks on a total of 29 sites, information infrastructure such unauthorized penetration achieved by infringement of security measures implemented in the server that housed the target Web sites.

Criminal activity led to total or partial compromise of Internet sites and areas covered, resulting in significant costs to recover data and implement new security measures.

At the D.I.I.C.O.T. will be brought to hear 12 people, to which research is carried out for crimes without the right to access information systems in order to obtain computer data in violation of security measures, modification of computer data without right and unauthorized transfer of data a computer system provided. of art..Article 42. 1, 2, 3 and art. Article 44. 1, 2 of Law no. 161/2003.

The investigations were carried out with the judicial police officers in DCCO. - S.C.C.I. and Special Operations Division.

The action was carried out with the support of the Romanian Gendarmerie.

Technical support and information was provided by SRI.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36J55T41/NSICG

Comunicat de presă - 29.05.2012

Marți, 29 Mai 2012 00:00



COMUNICAT DE PRESĂ

29.05.2012

Procurorii Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Structura Centrală au destructurat o grupare infracțională, constituită din 14 persoane, sens în care au efectuat 12 perchezitii domiciliare în municipiile București, Iași, Alba Iulia, Piatra Neamț, Cluj Napoca, Drobeta Turnu Severin, Arad, Craiova, Reșița și Târgu Mureș.

Liderul grupării a fost identificat ca fiind învinuitul BĂLĂEASA Gabriel, 24 de ani, din municipiul Piatra Neamț, cunoscut în mediul virtual cu nickname-urile „lulzcart, anonsboat, anonsweb, cartman”.

Acesta, împreună cu învinuitorii Fábián Gábor și Picoș Mihai Emil a constituit o grupare, la care au aderat și alte persoane, implicată în derularea agresiunilor de terorism cibernetic.

Gruparea a desfășurat o vastă activitate infracțională specifică, de criminalitate informatică, ce a constat în accesarea ilegală a sistemelor informatic, sustragerea de date confidențiale sau nedestinate publicitatii, precum și publicarea în mediul on-line a datelor exfiltrate.

Bazele de date confidențiale/clasificate vizate erau de predilecție administrate de instituții și persoane juridice publice, atât din România cât și din străinătate.

Din punct de vedere tehnic și al modalității concrete de operare, atacurile informatic lansate asupra serverelor și paginilor web întă, erau de tip SQL Injection, prin folosirea unor diferite aplicații informatic, respectiv Havij, SQL Map etc. În majoritatea cazurilor, după compromiterea și obținerea accesului neautorizat la site-urile vizate, membrii grupării aduceau modificări datelor informatic, executând atacuri de tip „Deface”, constând în introducerea unei pagini web în locul paginii principale a site-ului, modificare care constă în general în postarea anumitor mesaje, link-uri și imagini prin care se revendica atacul și se promova gruparea de hackeri.

Atacurile erau lansate în scopul obținerii de date informatic, date care erau după caz copiate/transferate fără drept și publicate ulterior în mediul virtual pe diverse site-uri, ca dovadă a activității de hacking.

Membrii grupării au procedat astfel la lansarea de atacuri informatic asupra unui număr de 29 de site-uri, pătrunderea neautorizată în respectivele infrastructuri informaționale realizându-se prin încălcarea măsurilor de securitate implementate la nivelul serverelor care găzduiau site-urile web întă.

Activitatea infracțională a dus la compromiterea totală sau parțială a paginilor și domeniilor de internet vizate, generând costuri semnificative în vederea recuperării datelor și implementării de noi măsuri de securitate .

La sediul D.I.I.C.O.T. vor fi aduse în vederea audierii 12 persoane, față de care se efectuează cercetări pentru săvârșirea infracțiunilor de acces fără drept la sisteme informative, în scopul obținerii de date informative prin încălcarea măsurilor de securitate, modificare fără drept de date informative și transfer neautorizat de date dintr-un sistem informatic, prev. de art. 42 alin. 1, 2, 3 și art. 44 alin. 1, 2 din Legea nr. 161/2003.

Cercetările au fost efectuate împreună cu ofițeri de poliție judiciară din cadrul D.C.C.O . – S.C.C.I. și Direcția Operațiuni Speciale.

Acțiunea a fost efectuată cu sprijinul Jandarmeriei Române.

Suportul tehnic și informativ a fost asigurat de către SRI.

FD-340 (Rev. 4-11-03)

File Number 288A-JK-53354

Field Office Acquiring Evidence JK

Serial # of Originating Document _____

Date Received 5/30/12

From

(Name of Contributor/Interviewee)

b7D

(Address)

FL 34230

(City and State)

By S.A.

b6

b7C

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

Letter from for shipment of evidence.

CART Request

b7D

CART Exam Service Request Confirmation - 1A Material

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36J55T41/NSICG

Your Exam service request has been entered into the system and is pending review by the JK office. A representative from the JK office will contact you shortly regarding the status of your request with further information and instructions.

Service Request ID: 45405
Request Type: Exam
Request Date: 05/30/2012
Request Priority: 2 (Priority)
Requested Completion Date: 06/08/2012
Investigative Request? Yes
UCFN: 288A - JK - 53354
Case Agent/Investigator: SA [redacted]
Case Agent/Investigator Field Office: JK
Case Agent/Investigator Supervisor: SSA [redacted]
Case Title: UNSUB (S); LAKE COUNTY SHERIFF'S OFFICE - VICTIM
Case Synopsis: On 21 April 2012 [redacted] notified LEGAT Bucharest that [redacted]

b6
b7C

b7D

Submitting Agency: JK
Agency Case/File Number:
Contact Information: 904-2487214
Assign Request To: JK
Evidence to be Examined:
Request Description: copy media and give to SA and return originals to evidence.
Legal Authority: Consent

FD-340 (Rev. 4-11-03)

File Number 288A-JK-53354

Field Office Acquiring Evidence JK

Serial # of Originating Document _____

Date Received 5/31/12

From Lake County Sheriff's office,
(Name of Contributor/Interviewee)

360 West Ruby Street,
(Address)

Tavares, FL, 32778
(City and State)

By SA

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Title:

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

b6
b7C

b6
b7C

b7D

FD-340 (Rev. 4-11-03)

IA 11

File Number 788A-SK-53354

Field Office Acquiring Evidence Sk

Serial # of Originating Document 37

Date Received _____

From: SA Name of Contributor/Interviewee)

b6
b7c

(Address)

(City and State)

By AECT

To Be Returned Yes No

Receipt Given Yes No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

Yes No

Federal Taxpayer Information (FTI)

Yes No

Title:

Reference: _____
(Communication Enclosing Material)

Description: Original notes re interview of

Orig C&C & FD-192 for
IB1 and IB2.

04/25/12
16:16:22

FD-192

ICMIPR01
Page 1

Title and Character of Case:

LAKE COUNTY SHERIFFS OFFICE

Date Property Acquired: Source from which Property Acquired:

04/25/2012

360 W RUBY STREET
TRAVORES FL 32778

LCSO

b6
b7C

Anticipated Disposition: Acquired By: Case Agent:

Description of Property:

1B 1

Date Entered

WESTERN DIGITAL MY BOOK STUDIO EXTERNAL HARD DRIVE,
SN: WCAZA3188836 (2TB,W/POWER SUPPLY & USB CABLE)
CONTAINING: BACKUPS & IMAGES OF LEO APP1, LEO CITRIX,
APP2(LEO TTA), AS WELL AS LOGS FROM LEO APPL, LEOCITRIX,
LEOASP1,WEBSITE LOGGING

Barcode: E4725431

Location: ECR

CART

BIN14

04/25/2012

Case Number: 288A-JK-53354
Owning Office: JACKSONVILLE

PACKAGE
COPY

FEDERAL BUREAU OF INVESTIGATION
EVIDENCE CHAIN-OF-CUSTODYEvidence Type: General
 CART Drug
 Valuable Firearm/Weapon
 Firearm/Other

Special Handling Instructions		Initial Receipt	Date and Time
<input type="checkbox"/> Batteries <input type="checkbox"/> Biohazard <input type="checkbox"/> FGJ <input type="checkbox"/> HAZMAT <input type="checkbox"/> Latents <input type="checkbox"/> Refrigerate <input type="checkbox"/> Req. Charging <input type="checkbox"/> None <input type="checkbox"/> Other		Signature _____ Printed Name: _____ Reason: Collected	4/25/2012 10:00 AM b6 b7c
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: _____ Printed: _____ Reason: To storage	4/25/2012 4:04 pm	Signature: _____ Printed Name: _____ Reason: Otonago	4-25-12 404 p
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: _____ Printed Name: _____ Reason: (O) CART	5-2-12 945 A	Signature: _____ Printed Name: _____ Reason: CART	5/2/12 945 AM
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: _____ Printed Name: _____ Reason: storage	5/2/12 140 PM	Signature: _____ Printed Name: _____ Reason: storage	5/2/12 1:40 P
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: _____ Printed Name: _____ Reason: IAD per lead	2/21/13 12:45P	Signature: _____ Printed Name: _____ Reason: _____	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature: _____ Printed Name: _____ Reason: _____		Signature: _____ Printed Name: _____ Reason: _____	

Firearms Certification:

Printed Name: _____ Signature: _____ Date: _____
Case ID: 288A-JK-53354 1B: 1 Barcode: E4725431

EVIDENCE CHAIN-OF-CUSTODY

Continuation Page

Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 288A-JK-53354

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-29-2014 BY J36J55T41/NSICG

On (date) 4/25/2012

- item(s) listed below were:
- Received From
 Returned To
 Released To
 Seized

b6
b7C(Name) Lake County Sheriff's Office(Street Address) 360 West Ruby Street Tavares, FL 32778

(City) _____

Description of Item(s): Western Digital My Book Studio 2TB
containing Backups and Images of
leo app1
leo Citrix
APP2 (LEOTTA)
as well as logs from leo app1, leo citrix, leo Asp1, website
logging

Serial Number - WCAZ A3188836

Received By: Received From: b6
b7C

06/04/12
09:03:36

FD-192

ICMIPR01
Page 1

Title and Character of Case:

LAKE COUNTY SHERIFFS OFFICE
HTTP PASTEHTML COM VIEW BW2M4UWHB HTML

Date Property Acquired: Source from which Property Acquired:

b6

b7C

b7D

05/30/2012

Anticipated Disposition: Acquired By:

Case Agent:

b6

b7C

Description of Property:

Date Entered

1B 2

- 1.2: SEAGATE 1TB HDD, SN:W1D07MG6 (EXCHANGE LIVE ACQUISITION 4/30/12, SECOND ORIGINAL FORENSIC IMAGE)
- 2.2: SEAGATE 1TB HDD, SN:W1D06LAK (LOG SERVER_4/30/12, SECOND ORIGINAL FORENSIC IMAGE)
- 3.2: SEAGATE 500GB HDD, SN:9QM9T8PD (IMAGES FROM LCSO, LEOCITRIX, LEOAPP1, LEOTTA APP2, SECOND ORIGINAL FORENSIC IMAGE)
- 4.2: COMPACT DISK (CD), COPY OF LSCO-120490-4 CD REC'D FROM LCSO HELP DESK E-MAIL
- 5.2: SEAGATE 500GB HDD, SN:W1D072K7 (IMAGES FROM (USERS + DEPTS BACKUP FROM 3-31-12) SECOND ORIGINAL FORENSIC IMAGE)
- 6.1: SEAGATE 1TB HDD, SN:5VP9S0H9 (IMAGES FROM LSCO 5/7/12, ORIGINAL FORENSIC IMAGE)

Barcode: E4725693

Location: ECR

CART BIN 14

05/30/2012

Case Number: 288A-JK-53354
Owning Office: JACKSONVILLE

PACKAGE
COPY

FEDERAL BUREAU OF INVESTIGATION
EVIDENCE CHAIN-OF-CUSTODY

Evidence Type: <input type="checkbox"/> General			<input type="checkbox"/> Drug			<input type="checkbox"/> Firearm/Weapon			
<input type="checkbox"/> CART			<input type="checkbox"/> Valuable			<input type="checkbox"/> Firearm/Other			
Special Handling Instructions			Initial Receipt			Date and Time			
<input type="checkbox"/> Batteries <input type="checkbox"/> HAZMAT <input type="checkbox"/> Req. Charging <input type="checkbox"/> Other			<input type="checkbox"/> Biohazard <input type="checkbox"/> Latents <input type="checkbox"/> None			Signature: Printed Name: Reason: Collected			
						5/30/12 3:00 pm			
Relinquished Custody			Date and Time			Accepted Custody			Date and Time
Signature: Printed Name: Reason: Storage			5/30/12 3:34 pm			Signature: Printed Name: Reason: Storage			5/30/12 3:34 pm
Relinquished Custody			Date and Time			Accepted Custody			Date and Time
Signature: Printed Name: Reason: GTO (CART)			5-30-12 4:30 PM			Signature: Printed Name: Reason: CIMA			5/30/12 4:30 PM
Relinquished Custody			Date and Time			Accepted Custody			Date and Time
Signature: Printed Name: Reason: Storage			6/4/12 9:00 AM			Signature: Printed Name: Reason: Storage			6-4-12 9:00 AM
Relinquished Custody			Date and Time			Accepted Custody			Date and Time
Signature: Printed Name: Reason: To CART			6-7-12 2pm			Signature: Printed Name: Reason: CIMA			6/7/12
Relinquished Custody			Date and Time			Accepted Custody			Date and Time
Signature: Printed Name: Reason: storage			6/8/12 1:55 PM			Signature: Printed Name: Reason: storage			6/8/12 1:55 PM

Firearms Certification:

Printed Name: _____ Signature: _____ Date: _____
Case ID: 288A-JK-53354 IB: 2 Barcode: E4725693b6
b7c

EVIDENCE CHAIN-OF-CUSTODY

Continuation Page

Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:	2/21/13 12:45p	Signature:	
Printed Name:		Printed Name:	
Reason:		Reason:	
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:			
Reason:			
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:			
Reason:			
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:			
Reason:			
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:			
Reason:			
Relinquished Custody	Date and Time	Accepted Custody	Date and Time
Signature:		Signature:	
Printed Name:			
Reason:			

Case ID: _____ 1B: _____ Barcode: _____

b6
b7c

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/26/2012

On April 26, 2012 Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] connected to the Internet and navigated to the following Uniform Resource Locator (URL):

<http://pastehtml.com/view/bw2m4uwhb.html>

The resulting web page appeared to be a tree listing of the Lake County Sheriff's Office (LCSO) server files. The web page, if printed, would have been 194 pages in length; therefore, SA [redacted] saved the web page to a Portable Document Format file (PDF). SA [redacted] then captured a screen print of the top of the web page, scrolled to the bottom of the web page and captured another screen print.

The screen captures and web page content pdf were copied to a CDR and placed in an FD-340 1A envelope and added to the 1A section of the case file.

b6
b7Cb6
b7CInvestigation on 04/26/2012 at Jacksonville, FloridaFile # 288A-JK-53354-2 Date dictated Not dictatedby SA [redacted]b6
b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/30/2012

On 4/27/2012 [redacted] of the Lake County Sheriff's Office (LCSO) at 360 West Ruby Street, Tavares, Florida 32778 was contacted telephonically to discuss the investigation into the LCSO network intrusion. Writer informed [redacted] that data related to the intrusion had been placed on-line at the Uniform Resource Locator (URL) <http://pastehtml.com/view/bw2m4uwhb.html>. The resulting web page appeared to be a directory tree listing of the LCSO files. The web page, if printed, would have been 194 pages in length and contained the names of directories and files that may have been exfiltrated from the LCSO network. It was later learned that four (4) files were posted to pastebin.com which were named Cyber Crime.zip, 911 Calls.zip, Swat Team Files.zip and Full Dump With Even More files then above.zip. Writer downloaded the above referenced files which were over 4.7 GB of data. [redacted] said that he would report the posting of the data to his command staff.

b6
b7C

During the night of 4/27/2012 [redacted] contacted writer again multiple times about email that was sent out to all the users on the LCSO network from the hackers. The email informed all the users that received the email that the LCSO network had been hacked. Writer again informed [redacted] that it was safe to assume that the entire LCSO network was compromised and that proper incident response and remediation should be undertaken by an outside firm. [redacted] asked if Writer could recommend any good groups to which Writer gave [redacted] a list of IT consulting firms. [redacted] said that they had changed all the passwords that they believed were compromised but that obviously did not work. He stated he would brief his command staff again and emphasize the severity of the situation and the need to have an external professional team come in and conduct the proper incident response and mitigation.

b6
b7C

On 4/28/2012 [redacted] met with [redacted] which is a Cyber Security Firm located at [redacted]. [redacted] Writer reached out to contacts in the Tampa Division and was assured that [redacted] was a credible Cyber Security Firm. [redacted]

b6
b7C
b7DInvestigation on 4/30/2012 at Tavares, FloridaFile # 288A-JK-53354 -4

Date dictated _____

by SA [redacted]b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

S:\DRAFTS\ [redacted].121\p112.wpd

b6
b7C

Continuation of FD-302 of _____

, On 4/30/2012 , Page 2

[redacted] contacted Writer and provided his cell phone number [redacted] and office number [redacted] and said that they were taking steps to secure the LCSO network and would retain any and all evidence of the intrusion to assist in the on-going investigation. [redacted] believed that the intrusion was related to multiple other intrusions by the same group of hackers and had located several IP addresses that he believed went back to infrastructure controlled by the hackers.

b6
b7C

On 4/28/2012 [redacted] informed Writer by telephone that the Florida Department of Law Enforcement (FDLE) had contacted him because of some information they had received about the intrusion into the LCSO network. Writer spoke with [redacted] of FDLE and [redacted] for FDLE and coordinated the LE efforts.

b6
b7C

On 4/28/2012 [redacted] with the LCSO reached out telephonically to Writer about a possible press report that would be coming from a news team out of the Orlando area. The news team received a tip and was asking LCSO for a statement/interview. Writer contacted and briefed [redacted] of FBI Jacksonville on the situation. [redacted] contacted [redacted] and asked him to limit his comments if possible and would not object to mentioning the FBI if he and/or the Sheriff thought it would help. [redacted] of the Office of Public Affairs, National Press Office, FBI HQ was briefed on the situation and advised all to use the statement "We're aware of this report but cannot comment further."

b6
b7C

FBI HQ Cyber Criminal PM SSA [redacted] who has been working with Jacksonville on this intrusion was updated and advised of the current situation and continues to coordinate with FBI Jacksonville.

b6
b7C

Writer identified the following online reports about the intrusion:

news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml

paintsthefuture.com/lake-county-sheriffs-office-hacked-by-antisec-and-leaked-4-7-gb-of-stolen-data/

Continuation of FD-302 of _____, On 4/30/2012, Page 3

jimmy89vl.blogspot.com/2012/04/lake-county-florida-sheriffs-office.html

gnsec.com/modules/d3pipes/index.php?page=clipping&clipping_it71380

On 4/30/2012 [redacted] stated via telephone that they had collected images of drives and other evidence of the intrusion and believed that it involved three 3 people, 1 in the US, 1 in Moscow and 1 in the Ukraine.

on 4/30/2012 [redacted] was contacted telephonically and stated that the LCSO was in lock down mode with the email server and website down as well as other services and that they were working with [redacted] to review all systems and bring them up one at a time once they had been secured. [redacted] is currently collecting data related to the intrusion and copies will be made and provided to the FBI to support the ongoing investigation. News channel 9 reported the LCSO intrusion.

b6
b7Cb6
b7C
b7D

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/25/2012

On 4/23/2012 SA [] and SA [] of FBI JK met with [] of the Lake County Sheriff's Office (LCSO) at 360 West Ruby Street, Tavares, Florida 32778 to discuss information that was passed from FBI HQ on 4/21/2012 to SA [] about a possible computer intrusion by [] into the LCSO network.

b6
b7C

[] was interviewed about a potential intrusion into the LCSO network. [] stated that he had been contacted by an FBI Agent out of San Antonio (SA) and told of a possible computer intrusion into the LCSO back in January 2012. [] stated that he checked his systems and found no evidence of the intrusion and attempted multiple times to reach back out to the FBI SA with negative results.

b6
b7C

[] was asked about any new intrusions into the LCSO network and stated that there were un-successful attempts and provided logs and data to back up his conclusions. Writer and SA [] advised [] to look again for the possible intrusion by checking server logs and legitimate user accounts for unusual activity and gave him an overview of criminal hacking procedures and techniques. [] called Writer back on 4/23/2012 after the meeting to report that he had found a user account that was being accessed for illegitimate purposes and was going to continue the investigation. [] was given part of a database table that FBI San Antonio had provided to Jacksonville when Jacksonville had reached out and inquired about the January 2012 contact with LCSO after leaving the LCSO meeting.

b6
b7C

On 4/25/2012 Writer met with [] and other staff from the LCSO. LCSO was again informed that the FBI had an open ongoing investigation into the intrusion and was working with international partners. [] provided one (1) hard disk drive (HDD) that contained images of 3 virtual servers, logs and data related to the intrusion. [] was given a property receipt (FD-597) for the HDD and signed a consent to search computers form. The HDD was placed into evidence and a CART request was completed requesting the imaging of the drive. HQ was contacted and forwarded a case support request form for assistance in reviewing the HDD and data provided by LCSO.

b6
b7CInvestigation on 4/25/2012 at Tavares, FloridaFile # 288A-JK-53354 -5

Date dictated _____

by SA []b6
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 04/30/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [redacted]

Approved By: [redacted] [redacted] S/1112

Drafted By: [redacted] [redacted]

Case ID #: 288A-JK-53354 (Pending) - 4

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Synopsis: To update case.

Details: (U//~~FOUO~~) On 21 April 2012 [redacted] notified LEGAT Bucharest that [redacted]

(U//~~FOUO~~) FBI Jacksonville immediately notified LCSO of the suspected intrusion. On 23 April 2012 Jacksonville met with LCSO and provided them an overview of criminal hacking techniques. Shortly thereafter, LCSO identified an unauthorized user account being accessed for illegitimate purposes. LCSO was instructed to begin remediating the problem and capturing forensic evidence.

(U//~~FOUO~~) LCSO was unsuccessful in fully eradicating the malicious actors, and on 27 April 2012 the LCSO mail server was compromised and used to distribute a mass e-mail message alerting all system users to the intrusion activity. One of the recipients of the message was the Florida Department of Law

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

S:\DRAFTS\ [redacted]\121\0212.wpd

b6

b7C

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 04/30/2012

Enforcement (FDLE), the state's central law enforcement agency. Later the same day, Twitter user "EvilSecurity" tweeted links to approximately 4.7 GB of LCSO's data, as well as a username and password to an account on LCSO's mail server.

(U//~~FOUO~~) On 28 April 2012 the Romanian-owned website Softpedia reported the theft of 40 GB of data from LCSO. The breach was attributed to Operation AntiSec, a series of hacks performed by members of Anonymous and LulzSec. According to Softpedia, one of the hackers, presumably [REDACTED], claimed 35 GB of the stolen data consisted of law enforcement software applications. The remaining 5 GB, which was posted online, consisted of "everything stored in the office's internal network that could be considered of value," including cyber crime information, audio recordings of 911 calls, photographs and personal details of SWAT operators, subpoena records, and FBI Intelligence Bulletins.

Investigative Action Plan: (U//~~FOUO~~) Jacksonville is currently coordinating this investigation with LCSO, FDLE, FBI Phoenix, LEGAT Bucharest, and [REDACTED]. The following investigative activity is ongoing or anticipated.

- 1.
 - 2.
 - 3.
 - 4.
 - 5.
 - 6.
 - 7.
 - 8.
- ♦♦

b6
b7C

b7D
b6
b7C

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/01/2012

Lt. [redacted], Lake county Sheriff's Office (LCSO), Florida was interviewed by the Federal Bureau of Investigation (FBI) regarding a recent computer intrusion into LCSO. After being advised of the identity of the interviewing Agent and the nature of the interview, [redacted] provided the following information:

[redacted] contacted FBI Special Agent (SA) [redacted] and advised that she had gone through the files that they believe were compromised and identified a file named FBI UPDATE TARGETING OF PRISONERS FOR IDENTITY THEFT.pdf from 2010 and that it was unclassified. [redacted] is not aware of any classified information at the LCSO.

According to a conversation [redacted] had with Lt. [redacted] [redacted] who coordinates the LCSO S.W.A.T team, there were no FBI agent's personal information obtained.

b6
b7Cb6
b7Cb6
b7C

Investigation on 05/01/2012 at Jacksonville, Florida (telephonically)
File # 288A-JK-53354 - 7 Date dictated Not dictated
by SA [redacted]

b6
b7C

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/01/2012

[redacted] Lake
County Sheriff's Office (LCSO), Florida was interviewed by the Federal Bureau of Investigation (FBI) regarding a recent computer intrusion into LCSO. After being advised of the identity of the interviewing Agent and the nature of the interview, [redacted] provided the following information:

b6
b7C

[redacted] contacted FBI Special Agent (SA) [redacted]

[redacted]

[redacted]

b6
b7C
b7D

After receiving the email, several LCSO members contacted [redacted] to report the incident. [redacted] stated [redacted]

[redacted]

b6
b7C
b7D

Investigation on 04/27/2012 at Jacksonville, Florida (telephonically)
File # 288A-JK-53354 -8 Date dictated Not dictated
by SA [redacted] [redacted]

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

S:\DRAFTS\SPRUITT\122sp0212.wpd

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 5/02/2012

To: Cyber

Attn: CCU1, SA [redacted]

b6
b7C

CCU2, SSA [redacted]

SSA [redacted]

Jacksonville

Attn: SA [redacted]

SA [redacted]

International Operations

Attn: Eurasia Unit, SSA [redacted]

From: Bucharest

Contact: ALAT [redacted]

b6
b7C

Approved By: [redacted] [redacted]

Drafted By: [redacted] [redacted]

Case ID #: (U) 163K-BO-893 (Pending) ¹³
(U) 288A-JK-53354 (Pending) ⁹

Title: (U) Anonymous Romania

Synopsis: (/-/ROU X) [redacted]

b1
b3
b7D

[redacted] regarding the
Anonymous Romania hack into the Lake County Sheriff's Office.

~~Derived From: Multiple Sources~~
~~Declassify On: 20370502~~

Details: (/-/ROU X) On 4/21/2012, Bucharest was notified via
telephone [redacted]

b1
b3

(U) Legat Bucharest's coordination with the FBI's Cyber
Initiative and Resource Fusion Unit (CIRFU) previously identified
[redacted]

b6
b7C
b7E

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FOI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: (U) 163K-BO-893, 5/02/2012

[REDACTED]

b6
b7C
b7E

(U) On 4/21/2012, ALAT [REDACTED] contacted LCSO and notified the database administrator there, [REDACTED] e-mail [REDACTED] regarding the possibility of an intrusion. [REDACTED] acknowledged the notification and began conducting research to verify the intrusion.

b6
b7C

(//~~FOI~~ X) On 4/23/2012, Legat Bucharest [REDACTED]

b1
b3

(C)

[REDACTED]

~~CONFIDENTIAL//FOI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: (U) 163K-BO-893, 5/02/2012

(//~~ROU~~) A sample of the information posted by [redacted]
[redacted] related to the intrusion in the channel #romania [redacted]

{C}

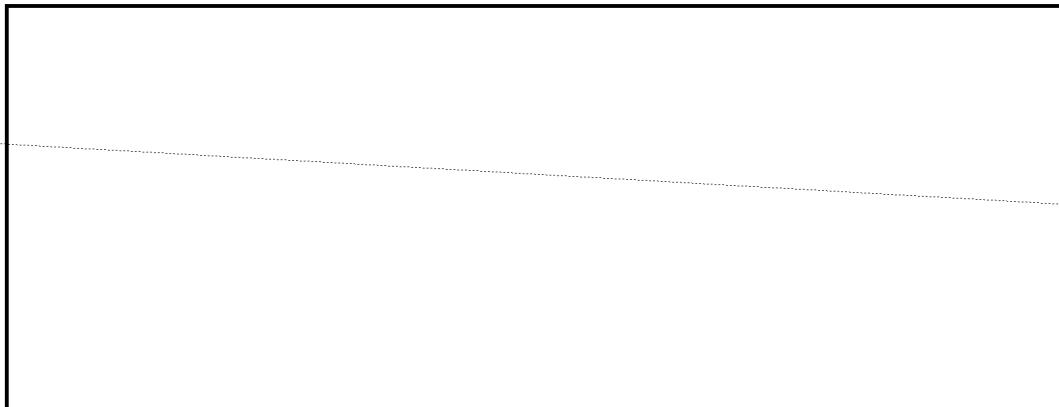


b1
b3
b6
b7c

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: (U) 163K-BO-893, 5/02/2012



b1
b3

(C)

(U) The information resulted in coordination with CyD and JK Division, resulting in the initiation of case 288A-JK-53354.

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: (U) 163K-BO-893, 5/02/2012

LEAD(s) :

Set Lead 1: (Info)

ALL RECEIVING OFFICES

(U) For information.

♦♦

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

Legat - Bucharest
Name: _____
Legal Attaché
U.S. Embassy - Bucharest
5260 Bucharest Place
Dulles, VA 20189

(011-40-21) 200-3339

FOR INTERNAL USE ONLY

~~CONFIDENTIAL~~

TO:

<input type="checkbox"/> Albany	<input type="checkbox"/> Houston	<input type="checkbox"/> Norfolk	<input type="checkbox"/> Abu Dhabi	<input type="checkbox"/> Jakarta	<input type="checkbox"/> Seoul
<input type="checkbox"/> Albuquerque	<input type="checkbox"/> Indianapolis	<input type="checkbox"/> Oklahoma City	<input type="checkbox"/> Amman	<input type="checkbox"/> Kabul	<input type="checkbox"/> Singapore
<input type="checkbox"/> Anchorage	<input type="checkbox"/> Jackson	<input type="checkbox"/> Omaha	<input type="checkbox"/> Ankara	<input type="checkbox"/> Kiev	<input type="checkbox"/> Sofia
<input type="checkbox"/> Atlanta	<input checked="" type="checkbox"/> Jacksonville	<input type="checkbox"/> Philadelphia	<input type="checkbox"/> Astana	<input type="checkbox"/> Kuala Lumpur	<input type="checkbox"/> Tallinn
<input type="checkbox"/> Baltimore	<input type="checkbox"/> Kansas City	<input type="checkbox"/> Phoenix	<input type="checkbox"/> Athens	<input type="checkbox"/> Lagos	<input type="checkbox"/> Tbilisi
<input type="checkbox"/> Birmingham	<input type="checkbox"/> Knoxville	<input type="checkbox"/> Pittsburgh	<input type="checkbox"/> Baghdad	<input type="checkbox"/> London	<input type="checkbox"/> Tel Aviv
<input type="checkbox"/> Boston	<input type="checkbox"/> Las Vegas	<input type="checkbox"/> Portland	<input type="checkbox"/> Bangkok	<input type="checkbox"/> Madrid	<input type="checkbox"/> Tokyo
<input type="checkbox"/> Buffalo	<input type="checkbox"/> Little Rock	<input type="checkbox"/> Richmond	<input type="checkbox"/> Beijing	<input type="checkbox"/> Manila	<input type="checkbox"/> Vienna
<input type="checkbox"/> Charlotte	<input type="checkbox"/> Los Angeles	<input type="checkbox"/> Sacramento	<input type="checkbox"/> Beirut	<input type="checkbox"/> Mexico City	<input type="checkbox"/> Warsaw
<input type="checkbox"/> Chicago	<input type="checkbox"/> Louisville	<input type="checkbox"/> Saint Louis	<input type="checkbox"/> Berlin	<input type="checkbox"/> Moscow	<input type="checkbox"/> _____
<input type="checkbox"/> Cincinnati	<input type="checkbox"/> Memphis	<input type="checkbox"/> Salt Lake City	<input type="checkbox"/> Bern	<input type="checkbox"/> Nairobi	
<input type="checkbox"/> Cleveland	<input type="checkbox"/> Miami	<input type="checkbox"/> San Antonio	<input type="checkbox"/> Bogota	<input type="checkbox"/> New Delhi	
<input type="checkbox"/> Columbia	<input type="checkbox"/> Milwaukee	<input type="checkbox"/> San Diego	<input type="checkbox"/> Brasilia	<input type="checkbox"/> Ottawa	
<input type="checkbox"/> Dallas	<input type="checkbox"/> Minneapolis	<input type="checkbox"/> San Francisco	<input type="checkbox"/> Bridgetown	<input type="checkbox"/> Panama City	
<input type="checkbox"/> Denver	<input type="checkbox"/> Mobile	<input type="checkbox"/> San Juan	<input type="checkbox"/> Brussels	<input type="checkbox"/> Paris	
<input type="checkbox"/> Detroit	<input type="checkbox"/> Newark	<input type="checkbox"/> Seattle	<input type="checkbox"/> Buenos Aires	<input type="checkbox"/> Prague	
<input type="checkbox"/> El Paso	<input type="checkbox"/> New Haven	<input type="checkbox"/> Springfield	<input type="checkbox"/> Cairo	<input type="checkbox"/> Pretoria	
<input type="checkbox"/> FBIHQ	<input type="checkbox"/> New Orleans	<input type="checkbox"/> Tampa	<input type="checkbox"/> Canberra	<input type="checkbox"/> Rabat	
<input type="checkbox"/> Honolulu	<input type="checkbox"/> New York City	<input type="checkbox"/> Washington Field	<input type="checkbox"/> Caracas	<input type="checkbox"/> Riyadh	
 	 	 	<input type="checkbox"/> Copenhagen	<input type="checkbox"/> Rome	
<input type="checkbox"/> Butte OSC	<input type="checkbox"/> Quantico (CIRG)	<input type="checkbox"/> Savannah OSC	<input type="checkbox"/> Dakar	<input type="checkbox"/> San Salvador	
<input type="checkbox"/> Clarksburg (CJIS)	<input type="checkbox"/> Quantico (Div. 2)	<input type="checkbox"/> Winchester (RMD)	<input type="checkbox"/> Doha	<input type="checkbox"/> Sanaa	
<input type="checkbox"/> Ft. Monmouth ITC	<input type="checkbox"/> Quantico (ERF)	<input type="checkbox"/> _____	<input type="checkbox"/> Freetown	<input type="checkbox"/> Santiago	
<input type="checkbox"/> Pocatello ITC	<input type="checkbox"/> Quantico (Lab)		<input type="checkbox"/> Hong Kong	<input type="checkbox"/> Santo Domingo	
			<input type="checkbox"/> Islamabad	<input type="checkbox"/> Sarajevo	

CLASSIFICATION LEVEL

(CHECK ONE)

UNCLASSIFIED - NOT SENSITIVE

UNCLASSIFIED - SENSITIVE

~~CONFIDENTIAL~~

SECRET

ATTENTION: SAC

~~CONFIDENTIAL~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/02/2012

To: Cyber

Attn: CCU1, SA [REDACTED]

b6
b7C

CCU2, SSA [REDACTED]

SSA [REDACTED]

— Jacksonville

Attn: SA [REDACTED]

SA [REDACTED]

International Operations

Attn: Eurasia Unit, SSA [REDACTED]

From: Bucharest

Contact: ALAT [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 163L-BO-893 (Pending)-14
288A-JK-53354 (Pending)-10

Title: ANONYMOUS ROMANIA

(C)

Synopsis: //~~ROU X~~ [REDACTED]

b1
b3
b7D

[REDACTED] regarding the
Anonymous Romania hack into the Lake County Sheriff's Office.

~~Derived From: Multiple Sources~~
~~Declassify On: 20370502~~

(C)

b1
b3

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/02/2012

(C)

b1
b3

(U) ALAT [REDACTED] provided the link to pastehtml.com to Jacksonville Cyber on 04/26/2012.

b6
b7c

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/02/2012

LEAD(s):

Set Lead 1: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Precedence:** ROUTINE**Date:** 05/02/2012**To:** Cyber**Attn:** UC [REDACTED]b6
b7C

CCU1, SA [REDACTED]

CCU2, SSA [REDACTED]

SSA [REDACTED]

Jacksonville

Attn: SA [REDACTED]

SA [REDACTED]

International Operations

Attn: Eurasia Unit, SSA [REDACTED]**From:** Bucharest**Contact:** ALAT [REDACTED]**Approved By:** [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 163L-BO-893 (Pending)¹⁵
288A-JK-53354 (Pending)-II**Title:** ANONYMOUS ROMANIA**Synopsis:** To document primary targets [REDACTED]

b7D

[REDACTED] CIRFU searches on the

Details: [REDACTED]b6
b7C
b7D

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/02/2012

[REDACTED]

b7D

ALAT [REDACTED] met with [REDACTED]

[REDACTED]

b7D

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/02/2012

LEAD(s):

Set Lead 1: (Action)

CYBER

AT CIRFU, DC

Conduct [redacted] and/or any other relevant checks for nicknames provided and coordinate any positive results with Bucharest and Jacksonville for [redacted]

b7D
b7E

Set Lead 2: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 3: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 4: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

UNCLASSIFIED

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/10/2012

To: Cyber

Attn: CCU1, SA [REDACTED]

b6
b7C

CCU2, SSA [REDACTED]

SSA [REDACTED]

Jacksonville

Attn: SA [REDACTED]

SA [REDACTED]

International Operations

Attn: Eurasia Unit, SSA [REDACTED]

From: Bucharest

Contact: ALAT [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 163L-BO-893 (Pending) -²⁰
288A-JK-53354 (Pending) -¹³

Title: ANONYMOUS ROMANIA

(C) Synopsis: (~~17 ROU X~~) [REDACTED]

b1
b3
b7D

[REDACTED] regarding members of
Anonymous Romania, reported hacks, and future targets.

Derived From: Multiple Sources
Declassify On: 20370510

b1
b3

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/10/2012

(C)

b1
b3

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/10/2012

(C)



b1
b3

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 05/10/2012

LEAD(s):

Set Lead 1: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

FD-515 (Rev. 8-30-2010)

Squad supervisor approval
(please initial)

Accomplishment Report

Date Prepared 5/29/12
Date Loaded 5/31/12
Date Loader's Initials _____

(Accomplishment must be reported and loaded into
ISRAA within 30 days from date of accomplishment)

Accomplishment Involves:
(check all that apply)

Drugs	<input type="checkbox"/>
A Fugitive	<input type="checkbox"/>
Bankruptcy Fraud	<input type="checkbox"/>
Computer Fraud/Abuse	<input checked="" type="checkbox"/>
Corruption of Public Official	<input type="checkbox"/>
Money Laundering	<input type="checkbox"/>
Sub Invest Asst by FO(s)	<input type="checkbox"/>

File Number	Q88A-JK-53354	
Stat Agent Soc. Sec. No.		
Stat Agent Name		
RA	Squad	/ /
Assisting Agents Soc. Sec. No. X	1	
Name:		
Assisting Agencies X •	2. - -	
Name:		

Investigative Assistance or Technique Used							
Rate FO	IAT	Rate FO	IAT	Rate FO	IAT	Rate FO	IAT
Fin. Analyst		Lab. Field Sup		UCO - Nat Back		Vict-Wtn Coor	
Aircraft Asst.		Pen Registers		NCAVC/V-CAF		IO Wanted Flyer	
Computer		Photo Cover		Crin/NS Intel Ass		SARs	
Consen Mon.		Polygraph		Cncls Neg.- Fed		CART	
ELSUR / FISC		Search Warrant		Crisis Neg - Local		Asset Forc Prog	
ELSUR / T. III		Show Money		ERT Asst.		Forc Support Prog	
Eng. Field Spt.		SOG Asst.		Butte - OSC		TFOS/CTD	
Eng. Tape Ex.		Swat Team		Sav - OSC		CXS/CTD	
Legats Asst.		Tech. Ag/Equip.		Poc - SC		InfraGard/CyD	
Evid. Purchase		Phone Toll Rec		Tech Rosp Unit		OFC/CID	
Int/CW Info		UCO - Group I		For. Lang Asst.		PPP	
Lab Div. Exam		UCO - Group II		Non FBI Lab Ex		Fusion Centers	

A. Complaint / Information/ Indictment

Federal Local International
Complaint Date: _____

Check if Civil Rico Complaint

Information Date: _____

Indictment Date: _____

F. Conviction

Federal Local International
Conviction Date: _____

Subject Description Code * (_____) *
For 6F, G, H-Include Agency Code

Felony or Misdemeanor
 Plea or Trial
State: _____ Judicial District: _____

J. Civil Rico Matters Date: _____
Also complete "Section G"
Other Civil Matters Date: _____
Judgment _____ *
Judicial Outcome _____ *
Amount \$ _____
Suspension: Years _____ Months _____

B. Locate / Arrest

Federal Local International
Subject Priority: A B C
Locate Date: 5/29/2012
Arrest Date: 5/29/2012
 Subject Resisted Arrest
 Subject Arrested was Armed

G. U.S. Code Violation
Required for sections A, B, F and J
(Federal Only)

Title	Section	# Counts
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

K. Administrative Sanction Date: _____
Subject Description Code _____
Type: _____ Length: _____
 Suspension Permanent
 Debarment or
 Injunction Year: _____ Months: _____

C. Summons Date: _____
 Federal Local

D. Recovery / Restitution / PELP X

Federal Local International
Recovery Date: _____
Code * _____ ✓ Amount \$ _____
Code * _____ ✓ Amount \$ _____
Restitution Date: _____
 Court Ordered Pretrial Diversion
Code * _____ ✓ Amount \$ _____
PELP Date: _____
Code * _____ ✓ Amount \$ _____

H. Sentence Date: _____
Sentence Type: _____ *
In Jail: Years _____ Months _____
Suspended: Years _____ Months _____
Probation: Years _____ Months _____
Fines: \$ _____

L. Asset Seizure Date: _____
Asset Forfeiture Date: _____
CATS # Mandatory _____
Circle below one of the three asset forfeiture:
Admin, Civil, Judicial, or Criminal
Do not indicate \$ value in Section D

M. Acquittal/ Dismissal/ Pretrial Diversion
(Circle one) Date: _____

E. Hostages(s) Released Date: _____
Released by: Terrorist Other
Number of Hostages: _____

I. Disruption/Dismantlement: ✓
Disruption Date: _____
Dismantlement Date: _____
Completion of FD-515a Side 2 Mandatory

N. Drug Seizures ✓ Date: _____
Drug Code * _____
Weight _____ Code * _____
FDIN _____
Do not indicate \$ in Section D

O. Child Victim Information
Child located / Identified Date: _____
 Living Deceased

P. Subject Information - Required for all blocks excluding block D (Recovery/PELP), blocks E, I, L and N

Name	Race*	Sex	Date of Birth	Social Security No. (if available)
	M			

For Indictments/Convictions only:

- Subject related to an LCN, Asian Organized Crime (AOC), Latin Organized Crime (LOC), Russian/Eastern European, Caribbean, or Nigerian Organized Crime Group - Complete FD-515a, Side 1 Blocks A-E mandatory, F-H as appropriate
 Subject related to an OCC/Drug organization, a VCMO Program National Gang Strategy target group, or a VCMO Program National Priority Initiative target group - Complete FD-515a, Side 1 Blocks A-C only.

* Additional information may be added by attaching another form or a plain sheet of paper for additional entries.

* See codes on reverse side.

✓ Requires that an explanation be attached and loaded into ISRAA for recovery over \$1 m and PELP over \$5 m, disruption, dismantlement, and drug seizures.

Serial No. of FD-515

15

b6
b7C

b6
b7C
b7E

b6
b7C

For Further Instructions See: MAOP, Part II, Sections 3-5 thru 3-5.3.
Revised 12-19-2006

PROPERTY CODES

01	Cash
02	Stocks, Bonds or Negot. Instruments
03	General Retail Merchandise
04	Vehicles
05	Heavy Machinery & Equipment
06	Aircraft
07	Jewelry
08	Vessels
09	Art, Antiques or Rare Collections
11	Real Property
20	All Other

SENTENCE TYPES

CP	Capital Punishment
JS	Jail Sentence
LP	Life Parole
LS	Life Sentence
NS	No Sentence (Subject is a Fugitive, Insane, has died, is a Corporation or must pay fine only)
PB	Probation
SJ	Suspension of Jail Sentence
YC	Youth Correction Act

PFLP CODES

22	Counterfeit Stocks/Bonds/Currency/ Negotiable Instruments
23	Counterfeit/Pirated Sound Recordings or Motion Pictures
24	Bank Theft Scheme Aborted
25	Ransom, Extortion or Bribe Demand Aborted
26	Theft From or Fraud Against Government Scheme Aborted
27	Commercial or Industrial Theft Scheme Aborted
30	All Other

RACE CODES

A	Asian/Pacific Islander
B	Black
I	Indian/American
U	Unknown
W	White
X	Nonindividual

AGENCY CODES

AFOSI	Air Force Office of Special Investigations
ACIS	Army Criminal Investigative Service
BATF	Bureau of Alcohol, Tobacco & Firearms
BIA	Bureau of Indian Affairs
CBP	Customs and Border Protection
DCAA	Defense Contract Audit Agency
DCIS	Defense Criminal Investigative Service
DEA	Drug Enforcement Administration
DOC	Department of Corrections
DOI	Dept. of Interior
DHS	Dept. of Homeland Security
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
HHS	Dept. of Health & Human Services
HUD	Dept. of Housing & Urban Development
ICE	Immigration and Customs Enforcement
IRS	Internal Revenue Service
NASA	Natl Aeronautics & Space Admin
NBIS	Natl Narc Border Interdiction
NCIS	Naval Criminal Investigative Service
RCMP	Royal Canadian Mounted Police
SBA	Small Business Administration
USCG	U.S. Coast Guard
USDS	U.S. Department of State
USMS	U.S. Marshals Service
USPS	U.S. Postal Service
USSS	U.S. Secret Service
USTR	U.S. Treasury
LOC	Local
CITY	City
COUN	County
ST	State
OTHR	Other

JUDGMENT CODES

CJ	Consent Judgment
CO	Court Ordered Settlement
DI	Default Judgment
DI	Dismissal
JN	Judgment Notwithstanding
MV	Mixed Verdict
SJ	Summary Judgment
VD	Verdict for Defendant
VP	Verdict for Plaintiff

JUDICIAL OUTCOME

AG	Agreement
BR	Barred/Removed
CC	Civil Contempt
DC	Disciplinary Charges
FI	Fine
PI	Preliminary Injunction
PR	Temporary Restraining Order
PS	Pre-filing Settlement
RN	Restitution
SP	Suspension
VR	Voluntary Resignation
OT	Other

SUBJECT PRIORITY

A	Subject wanted for crimes of violence, (i.e., murder, manslaughter, forcible rape) against another individual or convicted of such a crime in the past five years.
B	Subject wanted for crimes involving loss or destruction of property valued in excess of \$25,000 or convicted of such a crime in the past five years.
C	All other subjects.

DRUG CODES

COC	Cocaine
IILR	Heroin
IISH	Hashish
KAT	Khat
LSD	LSD
MAR	Marijuana
MDM	Methylenedioxymethamphetamine
MET	Methamphetamine
MOR	Morphine
OPM	Opium
OTD	Other drugs

DRUG WEIGHT CODES

GM	Gram(s)
KG	Kilogram(s)
L	Liter(s)
ML	Milliliter(s)
P	Plant(s)
DU	Dosage Unit(s)

SUBJECT DESCRIPTION CODES

ORGANIZED CRIME SUBJECTS

IF	Boss
JG	Underboss
III	Consigliere
JJ	Acting Boss
IK	Capodecina
IL	Soldier

KNOWN CRIMINALS

2A	Top Ten or LO, Fugitive
2B	Top Thief
2C	Top Con Man

FOREIGN NATIONALS

3A	Legal Alien
3B	Illegal Alien
3C	Foreign Official W/out Diplomatic Immunity
3D	U.N. Employee W/out Diplomatic Immunity
3E	Foreign Student
3F	All Others

TERRORISTS

4A	Known Member of a Terrorist Organization
4B	Possible Terrorist Member or Sympathizer

UNION MEMBERS

SD	President
SE	Vice-President
SF	Treasurer
SG	Secretary/Treasurer
SH	Executive Board Member
SI	Business Agent
SJ	Representative
SK	Organizer
SL	Business Manager
SM	Financial Secretary
SN	Recording Secretary
SP	Office Manager
SQ	Clerk
SR	Shop Steward
SS	Member
ST	Trustee
SU	Other

GOVERNMENT SUBJECTS

(6F, 6G, 6H)	Include Agency Code
6A	Presidential Appointee
6B	U.S. Senator/Staff
6C	U.S. Representative/Staff
6D	Federal Judge/Judge
6E	Federal Prosecutor
6F	Federal Law Enforcement Officer
6G	Federal Employee - GS 13 & Above
6H	Federal Employee - GS 12 & Below
6I	Governor
6K	Lt. Governor
6L	State Legislator
6M	State Judge/Judge

Continuation of GOVERNMENT SUBJECTS

6N	State Prosecutor
6P	State Law Enforcement Officer
6Q	State - All Others
6R	Mayor
6S	Local Legislator
6T	Local Judge/Judge
6U	Local Prosecutor
6V	Local Law Enforcement Officer
6W	Local-All Others
6X	County Commissioner
6Y	City Councilman

BANK EMPLOYEES

7A	Bank Officer
7B	Bank Employee

OTHERS

8A	All Other Subjects
8B	Company or Corporation

CHILD PREDATORS

9A	Child Care provider
9B	Clergy
9C	Athletic Coach
9D	Teacher/Aide
9E	Law Enforcement Personnel
9F	Counselor
9G	Relative
9H	Stranger
9I	Other

05/31/2012

***** ARREST *****

SENSITIVE / UNCLASSIFIED

Case Number: 288A-JK-53354
 Serial No.: 15

Stat Agent Name: [REDACTED]
 Stat Agent SOC.: [REDACTED]

Report Date: 05/31/2012
 Accom Date.: 05/29/2012

b6
 b7C

Does Accomplishment Involve	Assisting Joint Agencies	Assisting Agents SOC	Subject Name	
Drugs : N	[REDACTED]	[REDACTED]	[REDACTED]	b6
A Fugitive. : N	[REDACTED]	[REDACTED]	[REDACTED]	b7C
Bankruptcy Fraud. : N	[REDACTED]	[REDACTED]	[REDACTED]	
Computer Fraud/Abuse. : Y	[REDACTED]	[REDACTED]	[REDACTED]	
Corruption of Public Officials: N	[REDACTED]	[REDACTED]	[REDACTED]	
Money Laundering. : N	[REDACTED]	[REDACTED]	[REDACTED]	

RA Squad Task Force

 HQ 11

Sub. Invest. Asst by Other FOs:

1 = Used, but did not help
 2 = Helped, Minimally
 3 = Helped, Substantially
 4 = Absolutely Essential

b7E

Investigative Assistance or Technique Used				
FINAN ANALYST	LAB FIELD SUP	UCO - NAT BACK	VICT-WITN COOR	
AIRCRAFT ASST	PEN REGISTERS	NCAVC/VI-CAP	IO WANTED FLYR	
COMPUTER ASST	PHOTO COVERGE	CRIM/NS INTEL	SARS	
CONSEN MONITR	POLYGRAPH	CRIS NEG-FED	CART	
ELSUR/FISC	SRCH WAR EXEC	CRIS NEG-LOC	ASSET FORF PRO	
ELSUR/III	SHOW MONEY	ERT ASST	FORF SUPPORT P	
ENG FIELD SUP	SOG ASST	BUTTE OSC	TFOS/CTD	
ENG TAPE EXAM	SWAT TEAM	SAV OSC	CXS/CTD	
LEGATS ASST.	TECH AG/EQUIP	POC SC	INFRAGARD/CYD	
EVIDNCE PURCH	TEL TOLL RECS	FT. MON-NRCSC	OFC/CID	
INFORMANT/CW	UCO-GROUP I	FOR LANG ASST	PPP	
LAB DIV EXAMS	UCO-GROUP II	NON FBI LAB EX	FUSION CENTERS	

Arrest is for Federal, Local, or International (F/L/I).. : I

Arrest Subject Priority (A/B/C)..... : C

Did Subject Resist (Y/N)..... : N

Was Subject Armed (Y/N)..... : N

United States Code Violation

Title	Section	Count
-----	-----	-----

Accomplishment Narrative



Embassy of the United States of America

Office of Legal Attaché
Bucharest, Romania

File No. 163L-BO-893; 288A-JK-53354

1 June 2012

[Redacted]

b7D

RE: Anonymous Romania

Dear [Redacted]

[Redacted]
[Redacted]

b7D

[Redacted]

Yours truly,

[Redacted]

b6
b7C

SA [Redacted]
FBI
Legal Attaché
[Redacted]

By: SA [Redacted]
Assistant Legal Attaché

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/29/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [REDACTED]

b6
b7C

Approved By: [REDACTED] [REDACTED]

Drafted By: [REDACTED] [REDACTED]

Case ID #: 288A-JK-53354 (Pending) 17

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Synopsis: To update case on arrest of multiple individuals related to the above referenced investigation.

Details: (U//~~FOUO~~) On 5/29/2012 ALAT [REDACTED] advised thatb6
b7C
b7D(U//~~FOUO~~) [REDACTED]b6
b7C
b7D(U//~~FOUO~~) ALAT [REDACTED] provided a link to the official press release which was printed out and placed in a 1A and sent to the file.(U//~~FOUO~~) LCSO was contacted and advised of the arrest and stated that they will continue to coordinate with the FBI on any press releases they provide. [REDACTED]b6
b7C

b7D

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

S:\DRAFTS\ [REDACTED] 150 [REDACTED] 0312.wpd

b6
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 05/29/2012

[redacted] LCSO
has also provided [redacted]
copies of data from the intrusion which were shipped to FBI
Jacksonville on 5/25/2012.

b7D

♦♦

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(Rev. 05-01-2008)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/30/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [REDACTED]

Approved By: [REDACTED] [REDACTED]

b6
b7C

Drafted By: [REDACTED] [REDACTED]

18

Case ID #: 288A-JK-53354 (Pending)

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Synopsis: To document receipt of evidence.

Details: (U//~~FOUO~~) On 5/30/2012 Writer received two (2) shipments of evidence [REDACTED] relating to the above investigation. The two (2) shipments contained the following which were placed in evidence on 5/30/2012:

b7D

Item # Description

Item #	Description
[REDACTED]	

b7D

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

S:\DRAFTS\ [REDACTED] 151 [REDACTED] 0112.wpd

b6
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/31/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [REDACTED]

Approved By: [REDACTED] [REDACTED]

Drafted By: [REDACTED]

Case ID #: 288A-JK-53354 (Pending) 19

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIMSynopsis: (U//FOUO) To update case and claim statistical
accomplishments.Details: (U//FOUO) Writer has worked with the Lake County
Sheriff's Office [REDACTED]
[REDACTED][REDACTED] and a copy placed in a 1A and sent to the
file.b6
b7Cb6
b7C
b7D~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

S:\DRAFTS\ [REDACTED].152 [REDACTED] 0212.wpd

b6
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 5/31/2012

Accomplishment Information:

Number: 1

Type: CIP CASE [REDACTED]

ITU: CIP

Claimed By:

 SSN: [REDACTED]

 Name: [REDACTED]

 Squad: 11

b7E

b6

b7C

Number: 1

Type: CIP [REDACTED]

ARREST/SEARCH WARRANT CONDUCTED

b7E

ITU: CIP

Claimed By:

 SSN: [REDACTED]

 Name: [REDACTED]

 Squad: 11

b6

b7C

Number: 1

Type: CIP SUBJECT IDENTIFIED

ITU: CIP

Claimed By:

 SSN: [REDACTED]

 Name: [REDACTED]

 Squad: 11

b6

b7C

Number: 1

Type: CIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED

ITU: CIP

Claimed By:

 SSN: [REDACTED]

 Name: [REDACTED]

 Squad: 11

b6

b7C

Number: 1

Type: CIP VICTIM CONTACTED/INTERVIEWED

ITU: CIP

Claimed By:

 SSN: [REDACTED]

 Name: [REDACTED]

 Squad: 11

b6

b7C

Number: 1

Type: CIP CASE [REDACTED]

b7E

ITU: CIP

Claimed By:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 5/31/2012

SSN: [REDACTED]
Name: [REDACTED]
Squad: 11

b6
b7C

Number: 1
Type: CIP [REDACTED] ARREST/SEARCH WARRANT CONDUCTED
ITU: CIP
Claimed By:
SSN: [REDACTED]
Name: [REDACTED]
Squad: 11

b7E
b6
b7C

Number: 1
Type: CIP SUBJECT IDENTIFIED
ITU: CIP
Claimed By:
SSN: [REDACTED]
Name: [REDACTED]
Squad: 11

b6
b7C

Number: 1
Type: CIP SUBJECT TOOL/EXPLOIT/MALICIOUS CODE IDENTIFIED
ITU: CIP
Claimed By:
SSN: [REDACTED]
Name: [REDACTED]
Squad: 11

b6
b7C

Number: 1
Type: CIP VICTIM CONTACTED/INTERVIEWED
ITU: CIP
Claimed By:
SSN: [REDACTED]
Name: [REDACTED]
Squad: 11

b6
b7C

♦♦

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 06/04/2012

To: Jacksonville

From: Jacksonville

11

Contact: SA [redacted]

b6
b7C

Approved By: [redacted] [redacted]

Drafted By: [redacted] [redacted] [redacted]

Case ID #: 288A-JK-53354 (Pending) - 20

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIM

Synopsis: To document [redacted]

b7E

Details: (U//~~FOUO~~) On 5/30/2012 Writer received two (2) shipments of evidence [redacted] relating to the above investigation. The two (2) shipments contained the following which were placed in evidence on 5/30/2012:

b7D

Item # Description

--	--

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

S:\DRAFTS\ [redacted]\156\0212.wpd

b6
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 06/04/2012

(U//~~FOUO~~) CART made copies of the above media [redacted]

b7E

♦♦

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



Embassy of the United States of America

Office of Legal Attaché
Bucharest, Romania

File No. 163L-BO-893; 288A-JK-53354

6 June 2012

[Redacted]

b7D

RE: Anonymous Romania

Dear [Redacted]

[Redacted]
[Redacted]
[Redacted]

b7D

b7D

Yours truly,

A handwritten signature in black ink, appearing to read "John Doe".

SA [Redacted]
FBI

Legal Attaché

[Redacted]

By: SA [Redacted]
Assistant Legal Attaché

b6

b7C

Legat - Bucharest
Name: _____
Legal Attache
U.S. Embassy - Bucharest
5260 Bucharest Place
Dulles, VA 20189

(011-40-21) 200-3339

FOR INTERNAL USE ONLY

TO:

Albany Houston Norfolk
 Albuquerque Indianapolis Oklahoma City
 Anchorage Jackson Omaha
 Atlanta Jacksonville Philadelphia
 Baltimore Kansas City Phoenix
 Birmingham Knoxville Pittsburgh
 Boston Las Vegas Portland
 Buffalo Little Rock Richmond
 Charlotte Los Angeles Sacramento
 Chicago Louisville Saint Louis
 Cincinnati Memphis Salt Lake City
 Cleveland Miami San Antonio
 Columbia Milwaukee San Diego
 Dallas Minneapolis San Francisco
 Denver Mobile San Juan
 Detroit Newark Seattle
 El Paso New Haven Springfield
 FBIHQ New Orleans Tampa
 Honolulu New York City Washington Field

Butte OSC Quantico (CIRG) Savannah OSC
 Clarksburg (CJIS) Quantico (Div. 2) Winchester (RMD)
 Ft. Monmouth ITC Quantico (ERF) _____
 Pocatello ITC Quantico (Lab) _____

Abu Dhabi Jakarta Seoul
 Amman Kabul Singapore
 Ankara Kiev Sofia
 Astana Kuala Lumpur Tallinn
 Athens Lagos Tbilisi
 Baghdad London Tel Aviv
 Bangkok Madrid Tokyo
 Beijing Manila Vienna
 Beirut Mexico City Warsaw
 Berlin Moscow _____
 Bern Nairobi
 Bogota New Delhi
 Brasilia Ottawa
 Bridgetown Panama City
 Brussels Paris
 Buenos Aires Prague
 Cairo Pretoria
 Canberra Rabat
 Caracas Riyadh
 Copenhagen Rome
 Dakar San Salvador
 Doha Sanaa
 Freetown Santiago
 Hong Kong Santo Domingo
 Islamabad Sarajevo

CLASSIFICATION LEVEL

(CHECK ONE)

- UNCLASSIFIED - NOT SENSITIVE
 UNCLASSIFIED - SENSITIVE
 CONFIDENTIAL
 SECRET

ATTENTION: *SA*

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 06/14/2012

To: Jacksonville

From: Jacksonville

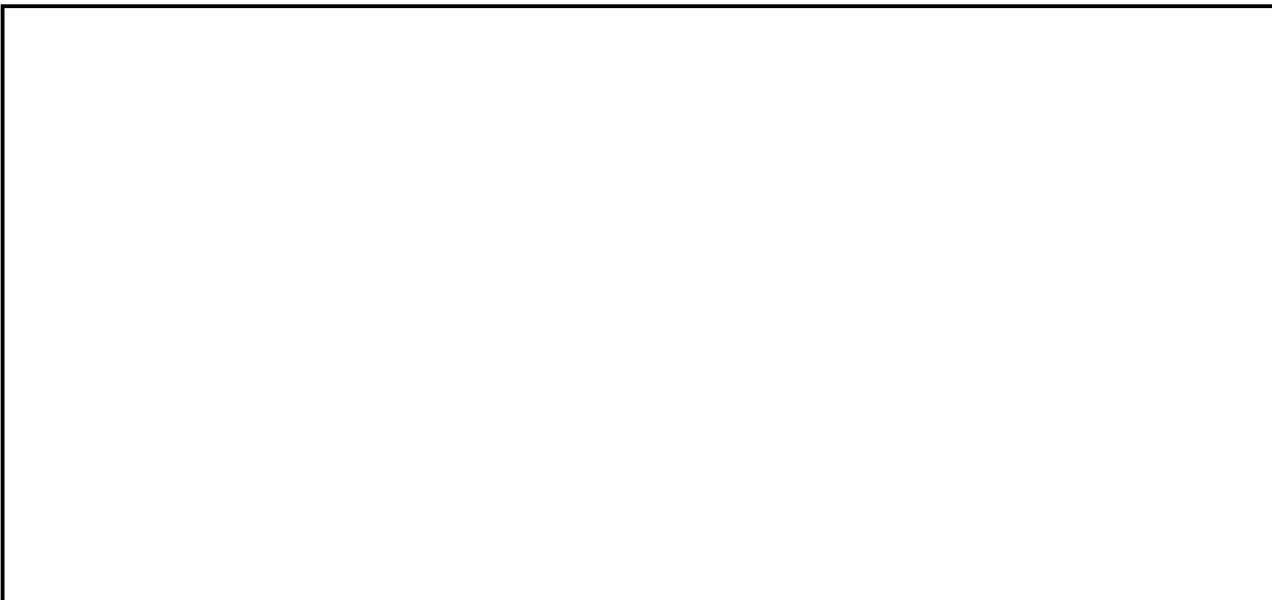
11

Contact: SA [REDACTED]

Approved By: [REDACTED] [REDACTED]

Drafted By: [REDACTED] [REDACTED]

Case ID #: 288A-JK-53354 (Pending) - 22

Title: UNSUB (S);
LAKE COUNTY SHERIFF'S OFFICE - VICTIMSynopsis: To document the receipt of a report [REDACTED]
[REDACTED] of data for the above referenced case for the period
6/4/2012 - 6/8/2012.Details: (U//~~FOUO~~) Writer received the following report from the
first part of the data analysis of the Lake County Sheriff's
Office data [REDACTED]A large rectangular area of the document has been completely redacted with black ink.~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

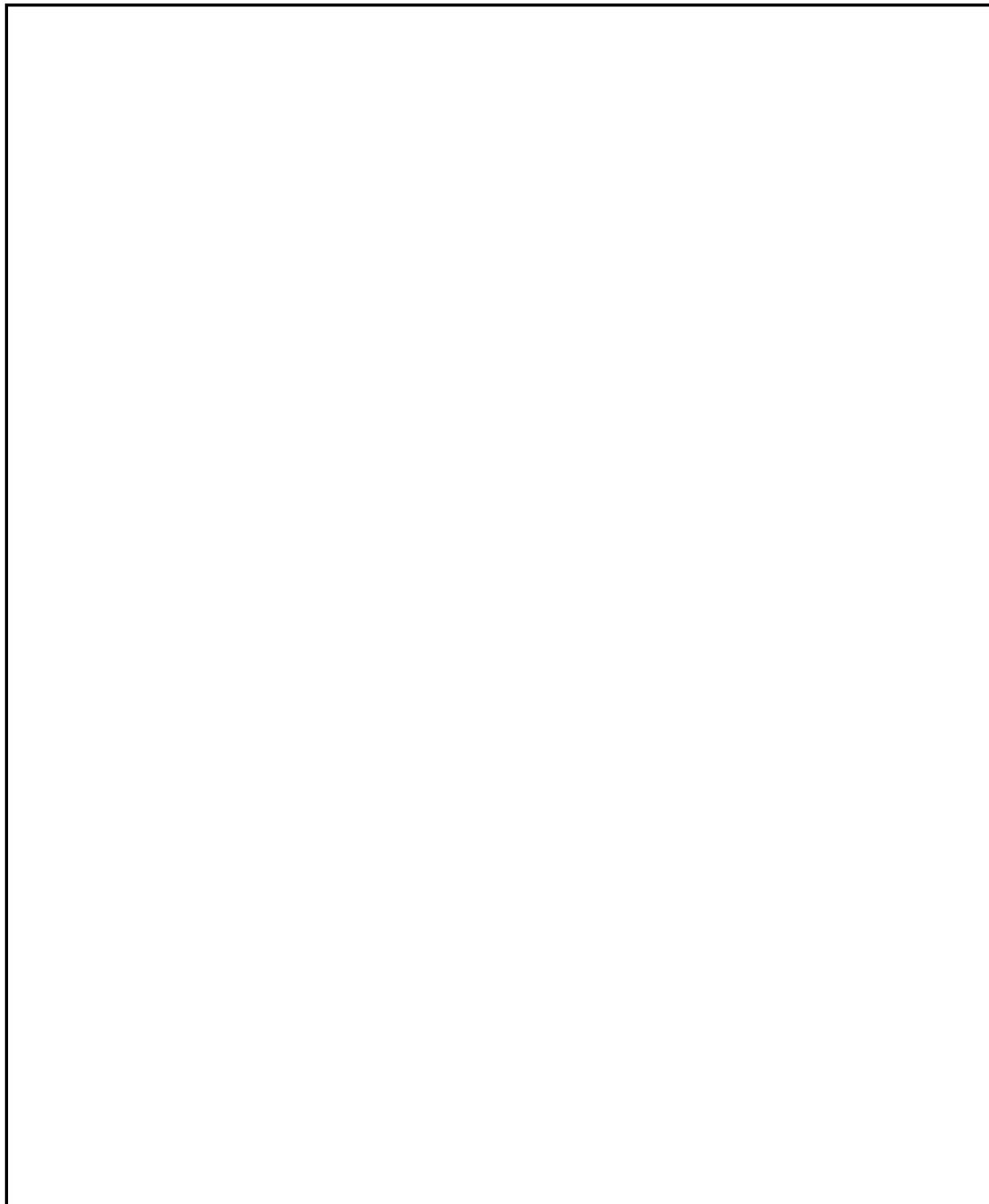
S:\DRAFTS\ [REDACTED]\166\0112.wpd

b6

b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 06/14/2012



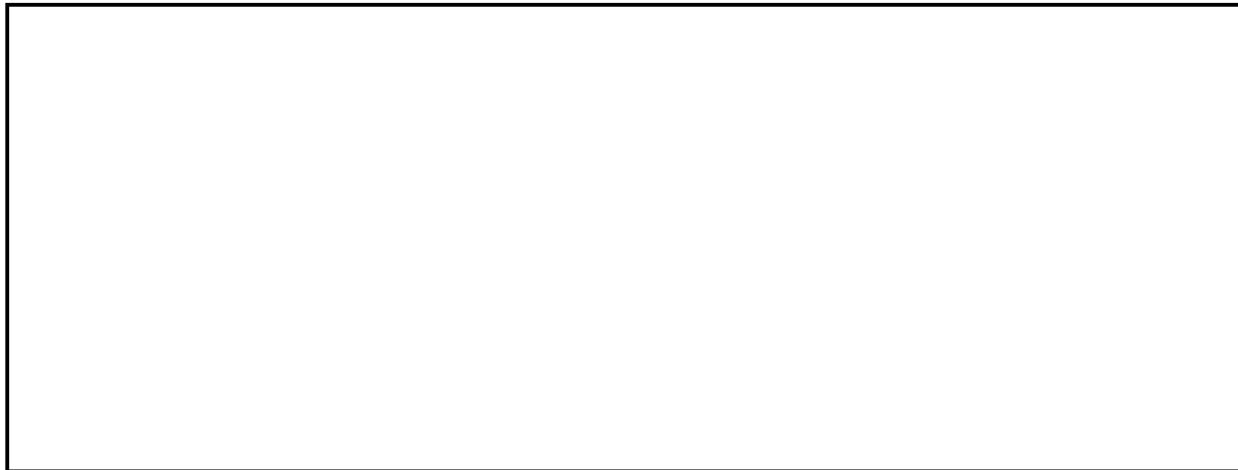
b6
b7C
b7E

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Jacksonville From: Jacksonville
Re: 288A-JK-53354, 06/14/2012

b7E



♦♦

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/26/2012

To: Cyber

Attn: CCU1, SA [redacted]

b6

CCU2, SSA [redacted]

b7C

Jacksonville

Attn: SA [redacted]

International Operations

Attn: SA [redacted]

Eurasia Unit, SSA [redacted]

From: Bucharest

Contact: ALAT [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 163L-BO-893

(Pending) -28

288A-JK-53354

(Pending) -25

Title: ANONYMOUS ROMANIA

Synopsis: //ROU (X) [redacted]

[redacted] regarding members of

Anonymous Romania.

b1

b3

b7D

Derived From: Multiple Sources

Declassify On: 20370627

b1

b3

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/26/2012

b1
b3

(C)



~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/26/2012

(C)

b1
b3

(U//~~FOUO~~) Cyber and Detroit divisions confirmed the hack related to Berrien, Michigan.

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/26/2012

LEAD(s) :

Set Lead 1: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

(Rev. 05-01-2008)

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/27/2012

To: Cyber

Attn: CCU1, SA [REDACTED] b6
CCU2, SSA [REDACTED] b7C

Jacksonville

Attn: IA [REDACTED]

International Operations

Attn: SA [REDACTED]

SA [REDACTED]

SSA [REDACTED]

Eurasia Unit, SSA [REDACTED]

From: Bucharest

Contact: ALAT [REDACTED]

Approved By: [REDACTED]

[REDACTED]

Drafted By: [REDACTED]

Case ID #: 163L-BO-893 (Pending) -²⁹
288A-JK-53354 (Pending) -²⁶

Title: ANONYMOUS ROMANIA

(C) Synopsis: //ROU (C) [REDACTED]

[REDACTED] regarding Anonymous Romania's members, activities, and plans.

b1

b3

b7D

Derived From : Multiple Sources

Declassify On: 20370627

b1

b3

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/27/2012

b1
b3

(C)

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/27/2012

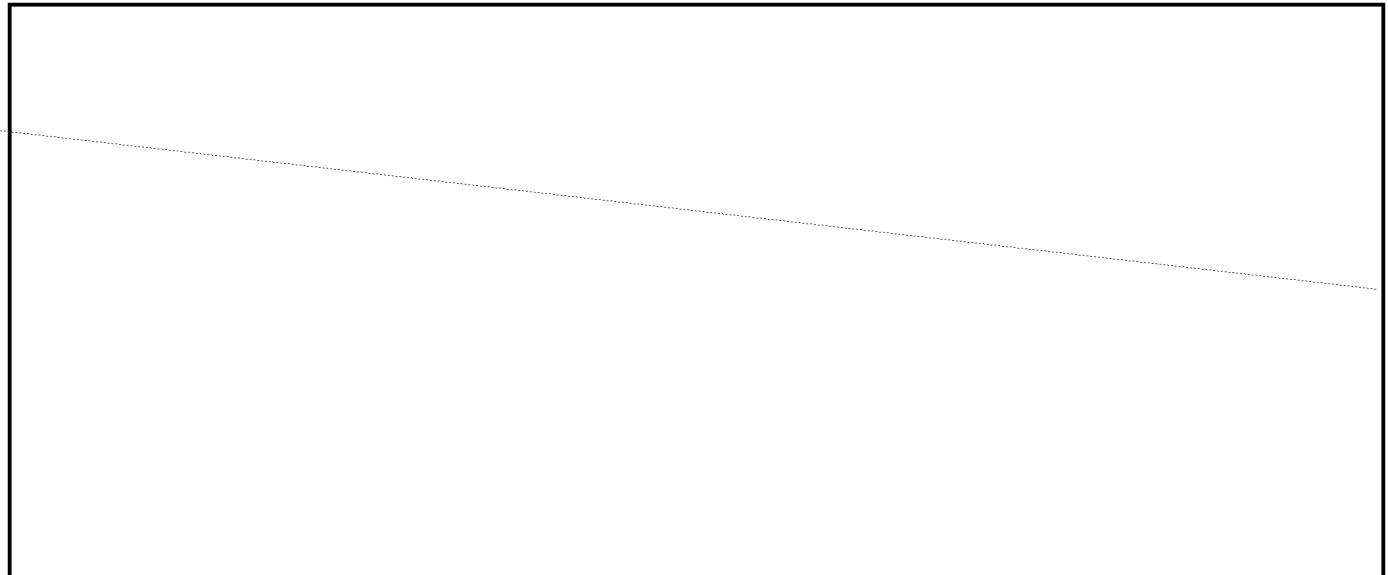
(C)

b1
b3

~~CONFIDENTIAL//FCI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/27/2012



b1
b3

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/27/2012

LEAD(s) :

Set Lead 1: (Action)

CYBER

AT PITTSBURGH, PA, CIRFU

Conduct searches of relevant datasets and provide any information on the channels #OpRomania and #tangodown. Also, provide any information on planned attacks on Romania due to the recent arrests of Anonymous Romania members if encountered.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

~~CONFIDENTIAL//FGI ROU/REL TO USA, ROU~~

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Precedence:** ROUTINE**Date:** 06/25/2012**To:** Cyber**Attn:** CCU1, SA [REDACTED]b6
b7C

CCU2, SSA [REDACTED]

Jacksonville

Attn: SSA [REDACTED]

International Operations

Attn: SA [REDACTED]**Attn:** Eurasia Unit, SSA [REDACTED]**From:** Bucharest**Contact:** ALAT [REDACTED]b6
b7C**Approved By:** [REDACTED]**Drafted By:** [REDACTED]Case ID #: 163L-BO-893 (Pending) -33
288A-JK-53354 (Pending) -21**Title:** ANONYMOUS ROMANIA**Synopsis:** Provide details of arrest and case update.**Details:** On 5/29/2012 [REDACTED]b6
b7C
b7D

[REDACTED] The prosecutor placed two of the subjects under arrest including the primary suspect implicated in the Lake County Sheriff's Office (LCSO) computer intrusion, [REDACTED] The other person arrested was [REDACTED]

On 5/31/12, [REDACTED]

b6
b7C
b7D

Although Legat Bucharest would have liked to work towards [REDACTED] extradition to the United States to face prosecution, due to the extradition treaty between Romania and the United States (US), he cannot be extradited until all legal proceedings in Romania, including the prison sentence, are complete. Once judicial authority has been requested in a

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/25/2012

Romanian investigation, such as a search warrant, the police are unable to pass the case to another jurisdiction for prosecution. Additionally, because Romania charged the LCSO in their indictment, extradition proceedings would face a more fundamental double-jeopardy issue in both the US and Romania.

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Bucharest
Re: 163L-BO-893, 06/25/2012

LEAD(s) :

Set Lead 1: (Info)

CYBER

AT CCU-1, DC

Read and clear.

Set Lead 2: (Info)

JACKSONVILLE

AT JACKSONVILLE, FL

Read and clear.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT EURASIA UNIT, DC

Read and clear.

♦♦

UNCLASSIFIED